STUDIO LEGALE MACELLO

SOCIETÀ TRA AVVOCATI

Politica per il Sistema di Gestione Integrato

Autore: Dr.ssa Cristina Caramellino

Approvatore: Avv. Debora Macello

Confidenzialità: L3

Data: 13/05/2024

Versione: 2.0

Sommario

1 Acronimi, definizioni e riferimenti

1.1 Acronimi

DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
HW	Hardware
ISO	International Standard Organization
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
SGI	Sistema di Gestione Integrato
SGQ	Sistema di Gestione della Qualità
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SOA	Statement of Applicability
SW	Software

1.2 Definizioni

SGI	SGQ + SGSI

1.3 Storia dei cambiamenti

Data	Versione	Note
2019	0.1-0.6	Stesura iniziale sotto forma di bozze non ufficiali.
19/01/2020	0.7	Riferimenti allineati agli altri documenti del SGI.
31/07/2020	1.0	Prima emissione per SGI.
31/03/2021	1.1	Aggiornamento post audit. Allineati riferimenti alle versioni di documenti correnti.
15/07/2021	1.2	Modifica frontespizio. Aggiunti autore, approvatore e livello di confidenzialità.
07/12/2021	1.3	Correzioni puntuali. Aggiunta di un punto al paragrafo 4.4 per sottolineare l'impegno dello Studio Legale al rispetto delle norme cogenti nell'ambito delle proprie attività. Aggiunti maggiori riferimenti ad elementi specifici dello Studio Legale lungo il documento.
15/06/2022	1.4	Correzioni puntuali. Aggiornamento paragrafo 6.4.1 con i documenti dell'analisi del rischio derivanti dal cambio di metodologia.
13/05/2024	2.0	Aggiornamento versione ISO/IEC 27001 da 2013 a 2022. Aggiornamento codici e nomi documenti di riferimento. Nessuna variazione sostanziale del contenuto.

1.4 Riferimenti

La presente Politica per il Sistema di Gestione Integrato è corredata dall'insieme di documenti specifici che indirizzano i vari processi a supporto; essi sono da intendersi come estensioni di applicazione puntuali e mandatori nei vari perimetri di applicazione. L'elenco completo è disponibile nel documento DOC 07.06 "Informazioni documentate di origine interna".

2 Introduzione

Il presente documento descrive la Governance adottata nello Studio Legale Macello (da qui in poi anche Studio Legale, Azienda o Organizzazione) per la costituzione di un Sistema di Gestione Integrato (SGI) al fine di garantire gli obiettivi relativi alla Qualità e alla Sicurezza delle Informazioni, in conformità anche con i requisiti e le strategie aziendali.

3 Scopo

L'implementazione di un Sistema di Gestione Integrato (Qualità e Sicurezza delle informazioni, secondo i requisiti delle norme ISO 9001:2015 e ISO/IEC 27001:2022) rappresenta un punto fondamentale per la crescita del business dell'Azienda, considerando la sua influenza su:

- Il preservare gli asset aziendali e le informazioni gestite (dati giudiziari, personali e comunque sensibili);
- Il rafforzamento del marchio dello Studio Legale;
- far crescere i profitti riducendo i costi ed ottimizzando le risorse;
- aumentare la fiducia e la soddisfazione dei clienti, garantendo un posizionamento di rilevanza dello Studio Legale sul mercato sia per ciò che attiene il core business dello Studio, ossia l'ambito dei servizi di recupero crediti giudiziale e stragiudiziale sia per ciò che attiene l'eventuale erogazione di nuove tipologie di servizi.

Pertanto, la definizione di una Politica di Gestione Integrata è un punto strategico per supportare e garantire gli obiettivi che possono essere raggiunti.

L'ambito giudiziario in cui opera lo Studio Legale impone non solo attenzione al rispetto delle norme cogenti ma anche costante implementenzione, aggiornamento e crescita dei processi aziendali. Il fine è di garantire la qualità dei servizi legali erogati ottimizzandone le performance e di massimizzare la tutela nella gestione dei dati trattati.

4 La Governance

4.1 Obiettivi della sicurezza

Lo Studio Legale si impegna a implementare la strategia per la Sicurezza delle Informazioni, basata sulla protezione della **riservatezza, integrità e disponibilità** di tutte le risorse informative fisiche e logiche dell'Azienda, al fine di garantire il rispetto dei requisiti normativi, operativi e contrattuali.

In particolare, gli obiettivi principali della Sicurezza delle Informazioni da affrontare sono:

- **Riservatezza:** garantire che le informazioni siano accessibili solo a coloro che sono autorizzati ad accedervi;
- **Integrità:** salvaguardia dell'accuratezza e della completezza delle informazioni e dei metodi di elaborazione;
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni quando necessario.

Gli obiettivi generali della Sicurezza delle Informazioni includono quanto segue:

- Garantire la conformità con le attuali leggi nazionali, i regolamenti (vedi MOD 07.05.01 “Documentazione di origine esterna - Elenco leggi”) e le linee guida, nonché le politiche interne dello Studio Legale;
- Stabilire controlli per proteggere i sistemi informativi e le informazioni dell’Organizzazione da furti, abusi e altre forme di danno e perdita;
- Motivare tutti i dipendenti a migliorare la loro consapevolezza della sicurezza al fine di proteggere e salvaguardare i dati dell’Azienda;
- Assicurarsi che lo Studio Legale sia in grado di dare continuità ai propri servizi, anche se si verificano incidenti di sicurezza importanti;
- Garantire la disponibilità e l'affidabilità dell'infrastruttura di rete e dei servizi forniti e gestiti dallo Studio Legale;
- Rispettare le metodologie degli standard internazionali per la Sicurezza delle Informazioni, in particolare quelle della norma ISO/IEC 27001:2022;
- Garantire flessibilità e un adeguato livello di sicurezza per l'accesso ai sistemi di informazione.

Il raggiungimento di questi obiettivi le attività e le iniziative di sicurezza, è monitorato periodicamente e rivisto durante il riesame della direzione. Lo Studio Legale definisce le attività, il proprietario e il manager, il risultato previsto, le risorse, i tempi e i metodi di misurazione dei risultati.

Lo Studio Legale prende in considerazione iniziative di sicurezza per:

- formazione e sensibilizzazione;
- analisi delle vulnerabilità tecniche;
- miglioramento dei controlli e dei relativi processi;
- aggiornamento della documentazione e delle procedure.

In ogni caso, la definizione di questi obiettivi è allineata con gli obiettivi strategici dello Studio Legale.

4.2 Obiettivi della Qualità

La Politica della Qualità dello Studio Legale ha quattro obiettivi principali:

OB1. mantenere sempre elevato il livello di soddisfazione degli stakeholder. Per quanto attiene i clienti questo avviene garantendo una costante formazione del personale ed investendo sull'innovazione tecnologica. Per quanto riguarda i fornitori l'obiettivo si raggiunge adottando, nella gestione delle relazioni, un atteggiamento trasparente ed empatico, garantendo parimenti condizioni economiche adeguate;
OB2. agevolare il processo partecipativo e di condivisione tra le proprie persone, in particolare dei dipendenti e dei collaboratori;
OB3. effettuare ogni valutazione sulla base di evidenze oggettive e nel rispetto delle norme e regolamenti in uso;
OB4. garantire la conformità e l'adeguatezza del servizio erogato al fine di aumentare la soddisfazione del cliente.

4.3 Strategia per la sicurezza

La visione della sicurezza dello Studio Legale si basa sulla protezione delle risorse informative, sulla gestione dei rischi per la sicurezza, sull'attuazione delle strategie di business in modo efficace ed efficiente, supportata da una leadership operativa e sostenuta da tutti i dipendenti dell'Organizzazione.

I principali driver coinvolti in una definizione del piano strategico di sicurezza sono:

- **Aspettative di sicurezza dello Studio Legale Macello:** l'aspettativa e l'ambizione dell'Organizzazione che sono l'input principale per definire i requisiti di sicurezza e l'investimento in una visione a lungo termine;
- **Gestione del rischio:** i risultati dal punto di vista della gestione del rischio per quanto riguarda i principali rischi per la sicurezza dell'Organizzazione in termini di Sicurezza delle Informazioni;
- **Regolamentazione e conformità:** influenza esterna attraverso esigenze normative e di conformità;
- **Esigenze e aspettative delle altre parti interessate:** rispondenza ai requisiti e soddisfazione del cliente;

- **Posizionamento rispetto alla sicurezza:** la posizione di sicurezza risultante dall'implementazione tecnologica messa in atto e dalle attività di verifica effettuate mediante gli audit periodici;
- **Campagne di sensibilizzazione:** i risultati delle campagne di sensibilizzazione che sono un indicatore della prontezza dei dipendenti in materia di sicurezza.

Questi driver e i relativi obiettivi devono essere stabiliti e rivisti ogni anno, al fine di considerarli come la base per una strategia a livello organizzativo e per impostare un corretto livello corretto per la Sicurezza delle Informazioni.

Devono essere noti sia la natura sensibile delle informazioni che l'Organizzazione memorizza e processa che il grave danno potenziale che potrebbe essere causato da incidenti di sicurezza che interessano tali informazioni; così come la violazione dei dati personali.

Ciò significa che la questione della sicurezza sarà considerata un'alta priorità nel prendere qualsiasi decisione commerciale. Ciò consentirà allo Studio Legale di allocare risorse umane, tecniche e finanziarie sufficienti alla gestione della Sicurezza delle Informazioni e di intraprendere azioni appropriate in risposta a tutte le possibili violazioni alla Sicurezza.

Gli impegni e gli sforzi aziendali per la sicurezza saranno:

- **Coordinati:** saranno prese misure di sicurezza basate su un quadro comune e tutto il personale sarà coinvolto nel mantenimento della conformità con esso;
- **Proattivi:** le minacce e le lacune di sicurezza saranno rilevate, identificate e gestite al fine di prevenire incidenti di sicurezza;
- **Supportati al massimo livello:** la sicurezza delle informazioni sarà supportata pienamente dal management per implementare i controlli di sicurezza identificati attraverso un processo di valutazione continuo del rischio.

4.4 Strategia per la Qualità

Sulla base dei principi generali di seguito esposti, sono state definite delle strategie con obiettivi misurabili che vengono monitorati in occasione dei riesami annuali da parte del Consiglio di Amministrazione, al fine di migliorare continuamente l'efficacia del SGQ, parte del SGI.

- Porre la massima attenzione nell'individuazione e nella soddisfazione delle esigenze delle proprie persone, in particolare dipendenti e collaboratori;
- Garantire la piena attuazione del Codice Etico Aziendale (DOC 05.02.03 "Codice Etico") al fine di assicurare il rispetto di tutti i principi basilari su cui esso si fonda e possono essere sintetizzati in trasparenza, etica e sostenibilità;
- Garantire l'impegno dello Studio Legale al rispetto delle norme cogenti (vedi MOD 07.05.01 "Documentazione di origine esterna - Elenco leggi" contenente un richiamo alle principali

norme cogenti) a cui lo Studio Legale deve attenersi, con particolare cura ed attenzione alle norme imposte per l'esercizio della professione forense;

- Migliorare continuamente la qualità della gestione della società e dei servizi offerti con la conseguente generazione di risultati positivi sia di natura economica sia in termini di eccellenza e reputazione verso l'esterno, con piena soddisfazione di clienti e partner;
- Ispirarsi ai principi di finanza etica nella conduzione delle relazioni economico-finanziarie con gli stakeholder e con le proprie persone;
- Garantire la disponibilità di professionalità sempre adeguate alle esigenze degli stakeholder e comunque del mercato di riferimento;
- Migliorare continuamente l'immagine di società responsabile ed efficiente;
- Mantenere alta l'attenzione ai principi di sostenibilità ambientale;
- Garantire una costante azione di valorizzazione, motivazione e crescita professionale delle persone;
- Rispettare i requisiti del SGQ e provvedere alla sua continua ed effettiva applicazione;
- Revisionare con continuità la Politica per garantire che le proprie persone, in particolare dipendenti e collaboratori, ne comprendano appieno i contenuti impegnandosi ad attuarli, e gli stakeholder siano sempre informati dell'evoluzione del contesto di riferimento della società.

4.5 Processo di Governance del SGI

Il framework adottato dallo Studio Legale e descritto in questo capitolo è ispirato al modello definito negli standard internazionali ISO che si riferiscono ai sistemi di gestione e che seguono lo schema HLS (High Level Structure); in particolare, la ISO 9001:2015 e la ISO/IEC 27001:2022 definiscono i requisiti "... per stabilire, implementare, operare, monitorare, revisionare, mantenere e migliorare un sistema di gestione della Qualità (SGQ) e della Sicurezza delle Informazioni (SGSI)".

Il modello descrive un approccio top-down che separa gli aspetti di governance (dichiarazioni, politiche e principi definiti dall'Organizzazione) dalla componente di management che riguarda il controllo dei processi di gestione della qualità e i controlli relativi alla sicurezza; il modello include un quadro di politiche e procedure che comprende tutti i controlli legali, fisici, tecnici e organizzativi coinvolti nei processi di gestione della qualità e del rischio delle informazioni di un'azienda.

La struttura del processo adottata in Azienda segue l'approccio di stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione per supportare la decisione strategica dell'Organizzazione di preservare la qualità dei propri prodotti/servizi e la riservatezza, l'integrità e la disponibilità delle informazioni in base alla struttura delle norme.

La Figura 1 riporta l'approccio adottato che consente peraltro di garantire un'integrazione efficace dei sistemi di gestione, dove il box relativo all'Annex A integra le componenti di sicurezza delle informazioni tipiche della ISO/IEC 27001 ai macro-processi comuni anche con la ISO 9001.

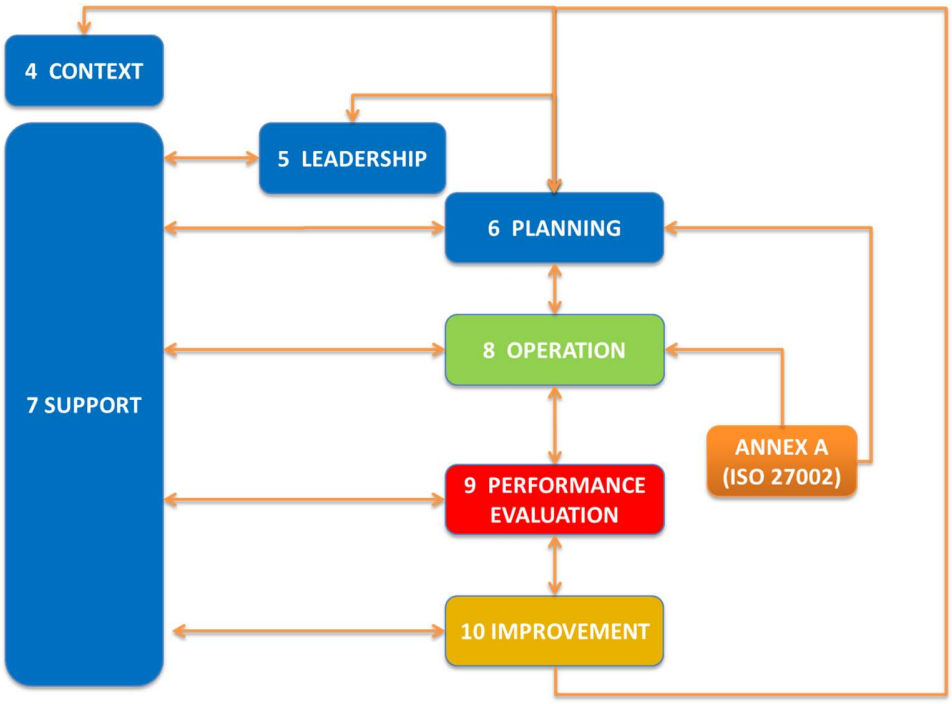

Figura 1 – capitoli della ISO/IEC 27001 e della ISO 9001 e integrazione dell'Annex A per la parte di sicurezza

Amministratori, dipendenti e collaboratori dello Studio Legale sono impegnati ogni giorno a perseguire gli obiettivi aziendali nel rispetto ed attraverso l'applicazione di un Sistema di Gestione e i criteri di sostenibilità ed etica aziendale.

Nello svolgimento delle proprie attività lo Studio Legale ha il compito di garantire:

- Un modello organizzativo aziendale in grado di assicurare sempre elevate e adeguate competenze tecnico scientifiche da applicare nel settore, garantendo anche i necessari livelli di riservatezza, integrità e disponibilità delle informazioni elaborate
- Stabilire ogni interazione con i propri clienti e partner con l'intento di creare valore, identificando al contempo esigenze presenti e future per il successo della società
- Un elevato livello di precisione procedurale e integrità delle professionalità coinvolte, mediante lo svolgimento di attività di ricerca o erogazione di servizi sempre e comunque conformi ai requisiti tecnici richiesti, alle procedure in uso, ai principi di etica e sostenibilità;

- La totale neutralità, indipendenza e imparzialità nei giudizi per garantire la massima obiettività di valutazione, la trasparenza e il rigetto di qualsiasi influenza o interferenza indebita sulle attività aziendali.
- Diffondere e comunicare a tutte le parti interessate identificate all'interno del contesto (vedere capitolo 5) la presente politica, gli obiettivi e le strategie con i dovuti dettagli in relazione all'effettivo coinvolgimento

Il SGI dello Studio Legale è improntato su un approccio di tipo risk-based, che consente all'organizzazione di determinare i fattori che potrebbero generare deviazioni dei processi rispetto alla norma ISO 9001:2015 e alla ISO/IEC 27001:2022, di mettere in atto controlli preventivi per minimizzare gli effetti negativi e cogliere al meglio le opportunità offerte dal mercato, anticipandone le tendenze. In aggiunta, nell'ambito della gestione della sicurezza delle informazioni, sono attuati controlli tecnologici e organizzativi sulla base dell'esito dell'analisi dei rischi che viene quindi periodicamente ripetuta e valutata.

Il Consiglio di Amministrazione s'impegna ad assicurare che questa Politica sia compresa, condivisa, implementata e attuata da tutti i propri dipendenti e collaboratori ed allo stesso tempo si impegna a condividerla con tutti gli stakeholder.

Il management dello Studio Legale opera a tutti i livelli con unità di intenti e obiettivi comuni, impegnandosi per creare le condizioni affinché dipendenti e collaboratori siano messi nelle condizioni migliori per raggiungere gli obiettivi fissati dal SGI. Tutto questo permette di allineare le strategie, i processi e le risorse per raggiungere gli obiettivi fissati dall'Azienda.

5 Contesto dell'Organizzazione

La descrizione del contesto dell'organizzazione è contenuta nel documento dedicato DOC 04.02 "Analisi del contesto".

6 Leadership

6.1 Leadership e impegno

La Politica Integrata dello Studio Legale nasce e si sviluppa come impegno della Direzione, questa si è evoluta attraverso l'operato della società intera, i requisiti specificati dalle norme ISO 9001:2015 e ISO/IEC 27001:2022 e le leggi in vigore applicabili all'attività giudiziaria dello Studio Legale. È pertanto intenzione dell'Azienda ottenere e mantenere la certificazione dei sistemi di Gestione Qualità e Sicurezza delle Informazioni, in quanto costituisce un fattore strategico di competitività e qualificazione sul mercato, nonché un'evidenza degli sforzi profusi dallo Studio Legale nel perseguire la continua soddisfazione di tutti i nostri clienti e partner.

La Direzione dello Studio Legale dimostra leadership e impegno nel rispetto della Qualità e della Sicurezza delle Informazioni attraverso:

- La stesura e revisione delle Politiche e Procedure Integrate;
- La struttura organizzativa formalizzata, con compiti e responsabilità definiti per quanto riguarda la gestione della Sicurezza delle Informazioni e della Qualità (vedi DOC 05.05 "Mansionario" e DOC 05.03 "Organigramma");
- La comunicazione al personale relativa alla necessità di soddisfare gli obiettivi, le politiche, i requisiti normativi e regolamentari applicabili (leggi, regolamenti, vedi MOD 07.05.01 "Documentazione di origine esterna - Elenco leggi")
- La pianificazione e la fornitura di risorse (sia materiali che umane, in termini di quantità e competenza);
- La definizione e la formalizzazione del livello di rischio e di accettabilità tramite opportuna analisi del rischio e analisi SWOT;
- La valutazione delle prestazioni della Sicurezza delle informazioni, della Qualità dei servizi erogati e l'efficacia della governance, tramite la definizione e la misurazione di appositi KPI;
- Le attività di audit interno;
- L'implementazione di riesami periodici.
- Il miglioramento continuativo rispetto agli obiettivi definiti e in relazione alle deviazioni derivanti da eventuali non conformità

6.2 Politica

La politica generale per la Qualità e per la Sicurezza delle Informazioni è riportata nel presente documento, con particolare riferimento ai requisiti delle norme ISO 9001:2015 e ISO/IEC 27001:2022. Riferirsi al documento MOD 07.05.01 "Documentazione di origine esterna - Elenco leggi" per l'insieme di norme e leggi cogenti che impattano i servizi forniti dallo Studio Legale.

6.3 Ruoli organizzativi, responsabilità ed autorità

Come riportato negli standard dello Studio Legale, le attività di Qualità e Sicurezza delle Informazioni sono coordinate e gestite da vari ruoli funzionali aziendali.

Le responsabilità, le autorità e i compiti relativi ai ruoli rilevanti per la Qualità e la Sicurezza delle Informazioni sono identificati all'interno della struttura aziendale.

I ruoli, le responsabilità e le autorità formalizzate sono rivisti dall'Azienda almeno una volta l'anno, nell'ambito del riesame del SGI, o secondo necessità.

L'organigramma, le responsabilità e le competenze relative ai componenti dello Studio Legale sono consultabili nei documenti DOC 05.03 "Organigramma" e "DOC 05.05 Mansionario".

6.4 Azioni per indirizzare i rischi e le opportunità

Lo Studio Legale definisce le sue priorità di governance della Sicurezza delle Informazioni e della Qualità attraverso un approccio di gestione del rischio (Risk Management): una visione di alto livello dell'approccio adottato è descritto nella sezione seguente.

6.4.1 Obiettivi del risk management

L'analisi del rischio è basata sugli asset individuati nel documento DOC.04.03.01 "Asset Inventory".

Riferirsi ai documenti:

- DOC 06.01.04 "Analisi SWOT" per l'analisi SWOT;
- DOC 04.03.01 "Asset Inventory" per l'elenco degli asset dello Studio Legale in ambito del SGI;
- DOC 06.01.02 "Metodologia Risk Assessment" per il metodo adottato per produrre il documento DOC 06.01.03 "Report Risk Assessment" e il DOC 06.01.06 "Piano di trattamento del rischio";
- DOC 06.01.03 "Report Risk Assessment" e il DOC 06.01.06 "Piano di trattamento del rischio" per le conclusioni derivanti dal processo di risk assessment.

6.4.2 Descrizione

Il Risk Management si basa su un framework che consente di identificare, valutare, notificare e monitorare il rischio delle informazioni in Azienda attraverso l'attività di valutazione del rischio.

Lo Studio Legale esegue le valutazioni del rischio in modo da identificare, quantificare e dare priorità ai rischi in base a criteri di accettabilità ben definiti e devono essere approvati dalla direzione.

Se una valutazione del rischio rivela rischi inaccettabili, l'Organizzazione implementa misure appropriate per ridurre il rischio a un livello accettabile.

6.4.3 Risk Management

Nel contesto dello Studio Legale, è stato compilato l'asset inventory dell'Azienda, catalogando i beni di natura HW e SW sulla base di:

- Funzione;
- Criticità;
- Impatti delle singole minacce.

Le minacce sono state determinate e valutate qualitativamente nell'ambito della stesura della DPIA e, successivamente, dettagliate, ampliate e valutate quantitativamente nell'ambito dell'analisi del rischio, espandendo le tipologie di eventi di disastro, pesandone impatto e verosimiglianza d'accadimento.

Dall'analisi quantitativa dei rischi sono state successivamente definite le azioni di risposta ai rischi, secondo impatti, criticità e probabilità.

Per i dettagli riferirsi ai documenti DOC 06.01.02 “Metodologia Risk Assessment”, DOC 06.01.03 “Report Risk Assessment e Trattamento” e DOC 06.01.06 “Piano di Trattamento del Rischio”.

6.4.4 Risorse

La disponibilità delle risorse è importante per garantire il raggiungimento degli obiettivi, pertanto lo Studio Legale definisce i piani opportuni per supportare il SGI. In particolare, l’Organizzazione considera:

- una pianificazione generale delle risorse;
- la coerenza tra pianificazione delle risorse in termini di quantità e piani di abilità/formazione;
- la tempestività nella disponibilità di risorse.

Al fine di mantenere elevata la capacità delle persone di svolgere correttamente il proprio lavoro e garantire il raggiungimento degli obiettivi previsti, sono effettuate le seguenti attività:

- Definire le competenze richieste per i ruoli relativi ai processi del SGI e agli aspetti di protezione dei dati e della Qualità;
- Definire ed erogare percorsi di formazione al fine di garantire le competenze necessarie e in particolare a qualsiasi persona che agisca sotto l'autorità dello Studio Legale (anche quando opera come titolare del trattamento dei dati), che ha accesso a dati personali;
- Verificare l'efficacia della formazione;
- Comunicare e condividere con tutto il personale l’insieme della documentazione dell’SGI tra cui la politica, il manuale e altre procedure operative;
- Creare la consapevolezza dell’importanza del proprio contributo e le implicazioni della mancata conformità ai requisiti di Qualità e Sicurezza delle Informazioni;
- Aumentare la risposta di tutto il personale ai rischi e agli incidenti di sicurezza.

6.4.5 Comunicazione

I documenti e le procedure relativi al SGI, laddove appropriato, forniscono istruzioni e criteri per comunicare, sia all'interno che all'esterno dell’Organizzazione, i risultati di varie attività: pertanto è stato predisposto un piano per la comunicazione all’interno del quale è stabilito come, quando e chi deve comunicare appropriate informazioni in relazione al contesto.

Il Piano di Comunicazione è redatto nel documento DOC 07.04 “Piano di Comunicazione”.

7 Attività Operative

Le attività operative sono orientate all'attuazione, all'applicazione di controlli specifici per identificare i rischi e mitigarli secondo le procedure e gli obiettivi di sicurezza e qualità definiti dalla direzione. L'organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i

requisiti per erogazione di servizi, inoltre deve assicurare che i processi affidati all'esterno siano tenuti sotto controllo.

Le attività sono definite dallo Studio Legale in specifici obiettivi di controllo e relative politiche e procedure atte ad indicare come tali obiettivi possono essere soddisfatti; analogamente sono fornite dallo Studio Legale indicazioni sugli strumenti adottati.

L'organizzazione deve assicurare che essa possiede la capacità di soddisfare i requisiti dei servizi da offrire ai clienti. Prima di impegnarsi a fornire tali servizi, l'organizzazione deve condurre un riesame sui requisiti richiesti, sia dal cliente, che dalle norme, che dai requisiti cogenti.

Gli obiettivi Sono strettamente allineati con i requisiti degli standard internazionali ISO/IEC 27001:2022 e ISO 9001:2015.

Il documento DOC 06.01.05 "SOA" (successivamente referenziato come SOA) riporta per ogni obiettivo di controllo definito nella norma ISO/IEC 27001:2022, la sua applicabilità nel contesto aziendale dello Studio Legale e le modalità con le quali tale obiettivo viene indirizzato, con particolare riferimento ai processi, alle politiche e alle procedure indicate nel documento DOC 07.06 "Informazioni documentate di origine interna".

Eventuali obiettivi aggiuntivi che dovessero essere utili o obbligatori per il mantenimento della sicurezza delle informazioni, quali ad esempio obblighi legali ed etica professionale, tipici dell'ambito di uno studio legale, saranno ugualmente riportati nella SOA.

8 Valutazione delle performance e miglioramento

Il monitoraggio delle attività di governance è orientato a valutare e misurare le prestazioni rispetto alla politica, agli obiettivi dell'Azienda e all'esperienza pratica. I risultati del monitoraggio sono uno degli input del riesame della direzione, e dimostrano come lo Studio Legale fornisca un'adeguata protezione delle informazioni e dei dati personali.

Lo Studio Legale deve monitorare la percezione del cliente riguardo al grado in cui le sue esigenze e aspettative sono state soddisfatte. L'azienda deve determinare i metodi per ottenere, monitorare e riesaminare queste informazioni.

L'Azienda, su base annuale, esegue audit sul Sistema di Gestione Integrato per valutarne l'effettiva attuazione e conformità. La pianificazione e la programmazione degli audit interni sono fornite e riviste in base ai risultati delle attività di monitoraggio. La frequenza degli audit interni è stabilita considerando il livello di rischio e le attività operative più critiche.

Lo Studio Legale monitora e misura l'efficacia dei controlli di sicurezza, il livello di soddisfazione dei clienti, i report degli audit interni, gli incidenti di sicurezza (compresa la violazione dei dati personali), le valutazioni e le risposte ai rischi. Il risultato delle attività di monitoraggio deve essere riportato ai

responsabili di competenza. A tal proposito lo Studio Legale definisce specifici indicatori di prestazione (KPI - Key Performance Indicator) e implementa uno specifico processo per valutare le performance dei processi e identificare le opportunità per il miglioramento del SGI. La revisione degli indicatori KPI viene eseguita durante il riesame della direzione.

Lo Studio Legale esegue un regolare Riesame della Direzione per garantire l'adeguatezza e la correttezza del SGI implementato. I risultati del riesame includono, tra gli altri, la revisione degli obiettivi di sicurezza e della qualità, oltre alla conferma del contenuto di questa politica di governance in base alla visione strategica aziendale.

Secondo i principi definiti dallo Studio Legale in questa politica, l'attenzione al miglioramento è dimostrata dal riesame di tutte le attività di monitoraggio (misurazione e audit interno) durante il Riesame della Direzione e l'analisi dei risultati conseguiti; per risolvere formalmente qualsiasi non conformità lo Studio Legale implementa opportune azioni correttive.

L'Azienda definisce un processo per il miglioramento continuo a partire dai risultati del monitoraggio e delle misurazioni. Mediante l'uso di uno specifico strumento di ticketing per registrare incidenti, le richieste di assistenza, le richieste di modifica (change) e problemi relativi al sistema di gestione integrato, possono emergere statistiche e proposte per aumentarne l'efficacia.

Lo strumento applicativo proprietario ReCre permette, tra l'altro, personalizzazioni e definizione di funzioni tali da poter essere utilizzato come strumento di ticketing per il tracciamento delle attività e degli eventi descritti qui sopra. Essendo lo strumento già utilizzato dallo Studio Legale per le proprie attività, ha in aggiunta il vantaggio di essere già familiare al personale.

Lo Studio Legale definisce gli obiettivi per migliorare la governance e le relative operazioni devono essere monitorate.

9 Politica di protezione dei dati personali a livello IT

La politica di protezione dei dati è un punto importante per le attività di trattamento dei dati personali, direttamente correlata alla sicurezza delle informazioni ed alla qualità dei servizi erogati. Lo studio Legale pianifica, identifica, implementa e gestisce attività specifiche al fine di dimostrare la sua responsabilizzazione ed il suo approccio.

Lo scopo di questa sezione della Politica è di delineare gli standard di conformità, i processi, le organizzazioni e le misure di controllo anche per la componente dei dati personali.

Pertanto, la politica indirizza i seguenti obiettivi:

- adottare un modello globale di protezione dei dati al fine di gestire correttamente i dati personali nel loro intero ciclo di vita;

- consentire a all'Azienda di far fronte alle responsabilità commerciali, legali e normative relative ai dati personali;
- aumentare la consapevolezza dei requisiti normativi, legali e aziendali per il trattamento e la protezione dei dati personali;
- stabilire una pratica aziendale chiara e completa per la gestione dei dati personali;
- stabilire la responsabilità per tutte le persone che gestiscono i dati personali;
- facilitare e consolidare pratiche comuni di gestione della privacy su base globale;
- mitigare i rischi (operativi, reputazionali e di conformità) relativi alla gestione e alla violazione dei dati personali;
- gestire correttamente la condivisione dei dati all'interno dell'Organizzazione l'accesso/trasferimento dei dati a terze parti.

Al fine di raggiungere gli obiettivi sopra definiti, lo Studio Legale adotta almeno i seguenti principi:

- trattare i dati personali in modo lecito, equo e trasparente (liceità, correttezza e trasparenza);
- trattare i dati personali in modo compatibile con finalità definite (limitazione delle finalità);
- elaborare i dati personali minimi necessari per scopi definiti (minimizzazione dei dati);
- elaborare dati personali aggiornati (esattezza);
- conservare i dati personali memorizzati per il tempo minimo necessario (limitazione della conservazione);
- elaborare i dati personali in modo tale da consentire al soggetto interessato di esercitare i propri diritti (efficacia);
- trattare i dati personali in modo tale da proteggere le informazioni (integrità e riservatezza);
- trattare i dati personali sotto la responsabilità e le disposizioni del titolare del trattamento dei dati (responsabilizzazione);
- consentire la rettifica o la cancellazione dei dati personali in risposta alla richiesta del soggetto a cui i dati fanno riferimento;
- considerare la privacy e la protezione dei dati dalla fase di progettazione (data protection by design) per la tecnologia, i sistemi e le attività operative al fine di garantire la privacy complessivamente;
- adottare un approccio basato sul rischio, considerando eventuali rischi per i diritti e le libertà dei soggetti a cui i dati fanno riferimento dovuti alle attività di trattamento dei dati svolte.